APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/645,459	08/20/2003	Manish Rathi	2717P100	8009

8791   7590   02/06/2009
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER
GERGISO, TECHANE

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
02/06/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/645,459	RATHI ET AL.
	Examiner	**Art Unit**	
	TECHANE J. GERGISO	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 November 2008*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *26-45* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *26-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   This is a Final Office Action in response to the applicant's communication filed on

November 24, 2008.

2.   Claims 26-45 have been examined and are pending.

Response to Arguments

3.   Applicant's arguments with respect to claims 26-44 have been considered but are moot in

view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

5.   Claims 26-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mukherjee

et al. (hereinafter referred to as Mukherjee, US Pub. No.: 2004/0006708 A1) in view of Cheline

et al. (hereinafter referred to as Cheline, US Pub No.: 2003/0041136 A1) and further in view of

Kwan et al. (hereinafter referred to as Kwan, US Pub. No.: 2004/0255154).

As per claim 26:

        Mukherjee discloses a method in a packet forwarder, comprising:

receiving a connection request from an unauthorized computing device at a first port of the

packet forwarder, the unauthorized computing device requesting access to a network

communicably interfaced with a second port of the packet forwarder (0050; Figure 4A:

404);

issuing the unauthorized computing device a first Internet Protocol (IP) address assigned to a

first Virtual Local Area Network (VLAN) operating within the packet forwarder and

associated with the first port, wherein the first VLAN does not provide access to the

network communicably interfaced with the packet forwarder via the second port, and

wherein the packet forwarder blocks the data packets in the first VLAN from reaching a

permanent VLAN that provides access to the network, the permanent VLAN operating

within the network and associated with the second port of the packet forwarder and not

the first port of the packet forwarder (Figure 2: 108; 0006; 0026; 0030; 0034);

sending the unauthorized computing device an authentication request through the first port of the

packet forwarder via the first VLAN based on the first IP address, responsive to the

connection request (0025; 0051; 0067);

authorizing the computing device based on satisfactory authentication credentials received from

the computing device via the first VLAN, responsive to the authentication request (0025;

0051; 0067); and

forwarding the data packets received from the authorized computing device at the first port of the

packet forwarder to the network via the second port of the packet forwarder using the

permanent VLAN based on the replacement IP address assigned to the authorized

computing device (0053; 0067).

Mukherjee does not explicitly disclose issuing the authorized computing device a replacement IP address assigned to the permanent VLAN for communication with the network, and associating the first port of the network forwarder with the permanent VLAN. Cheline, in analogous art however, disclose issuing the authorized computing device a replacement IP address assigned to the permanent VLAN for communication with the network, and associating the first port of the network forwarder with the permanent VLAN (0051; 0055; 0056; 0068; 0071). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Mukherjee to include issuing issuing the authorized computing device a replacement IP address assigned to the permanent VLAN for communication with the network, and associating the first port of the network forwarder with the permanent VLAN. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire to provide a computer implemented method for remotely configuring a Virtual Private Network (VPN) between a client-side system and a server-side system as suggested by Cheline (as suggested 0016).

Mukherjee and Cheline do not explicitly disclose blocking all data packets received at the first port of the packet forwarder from accessing the network. Kwan, in analogous art however, disclose blocking all data packets received at the first port of the packet forwarder from accessing the network (0038; 0039; 0071). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method

disclosed by Mukherjee and Cheline to include blocking all data packets received at the first port of the packet forwarder from accessing the network. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire to provide a network device that implements a multiple key, multiple tiered system and method for controlling access to a data communications network in both a single host and multi-host environment by providing a first level of security that comprises authentication of the physical (MAC) address of a user device coupled to a port of the network device, such as a network switch, a second level of security that comprises authentication of a user of the user device if the first level of security is passed, such as authentication in accordance with the IEEE 802.1x standard, and a third level of security that comprises dynamic assignment of the port to a particular VLAN based on the identity of the user if the second level of security is passed as suggested by Kwan in (0009) .

As per claim 27:

Mukherjee disclose a method, wherein receiving the connection request from the unauthorized computing device requesting access to the network comprises: intercepting a request from the unauthorized computing device for a web page (figure 5: IPSG router and VISA device).

As per claim 28:

Cheline disclose a method, wherein sending the unauthorized computing device the authentication request comprises: directing the unauthorized computing device to a network

login page for authentication, the network login page accessible on the first VLAN (figure 3B: 328, 331, 332).

As per claim 29:

Cheline disclose a method, wherein authorizing the computing device based on satisfactory authentication credentials from the computing device via the first VLAN, responsive to the authentication request comprises: receiving at least a user name and a password from the unauthorized computing device based on information captured by the network login page (figure 3B: 328, 331, 332; 334).

As per claim 30:

Cheline disclose a method, wherein directing the unauthorized computing device to the network login page for authentication comprises: responding to the unauthorized computing device with a redirect to a Uniform Resource Locator (URL) address for the network login page (0057).

As per claim 31:

Mukherjee disclose a method, further comprising: sending the authentication credentials to an authentication server; and receiving an indication from the authentication server that the authentication credentials are authentic and that a user associated with the authentication credentials is authorized to access the network (figure 4a: 408-418; 0025; 0039; 0051).

As per claim 32:

Cheline disclose a method, wherein sending the authentication credentials to the authentication server comprises: creating a packet comprising the authentication credentials in accordance with a Remote Authentication Dial-In User Service (RADIUS) communications protocol; and forwarding the packet to a RADIUS server for authentication, wherein the RADIUS server is accessible from the first VLAN (0043; 0044).

As per claim 33:

Mukherjee disclose a method, wherein the packet forwarder comprises a switch device located at an edge of the network to provide packet-forwarding services into the network (figure 1: 102).

As per claim 34:

Mukherjee disclose a method, further comprising:

terminating forwarding of the data packets between the authorized computing device and the network based on one or more events including (0035; 0052; 0064):

exceeding a pre-determined period of inactivity by the authorized computing device (0035; 0052; 0064);

receiving a reset signal is from a network login controller communicably interfaced with the data packet forwarder (0035; 0052; 0064);

receiving a termination command from an administrator account requesting forwarding of the data packets between the authorized computing device and the network be terminated;

determining a network connection between the authorized computing device and the

packet forwarder is disconnected (0035; 0052; 0064); and

determining a user of the authorized computing device has logged off of the computing device

(0035; 0052; 0064).

As per claim 35:

Mukherjee disclose a computer-readable medium having instructions stored thereon that,

when executed by a processor, cause the processor to perform a method comprising:

receiving a connection request from an unauthorized computing device at a first port of a

packet forward, the unauthorized computing device requesting access to a

network communicably interfaced with a second port of the packet forwarder

(0050; Figure 4A: 404);

issuing the unauthorized computing device a first Internet Protocol (IP) address assigned

to a first Virtual Local Area Network (VLAN) operating within the packet

forwarder and associated with the first port, wherein the first VLAN does not

provide access to the network communicably interfaced with the packet is

forwarded via the second port, and wherein the packet forwarder blocks the data

packets in the first VLAN from reaching a permanent VLAN that provides access

to the network, the permanent VLAN operating within the network and associated

with the second port of the packet forwarder and not the first port of the packet

forwarder (Figure 2: 108; 0006; 0026; 0030; 0034);

sending the unauthorized computing device an authentication request through the first

port of the packet forwarder via the first VLAN based on the first IP address,

responsive to the connection request (0025; 0051; 0067);

authorizing the computing device based on satisfactory authentication credentials

received from the computing device through the first port of the packet forwarder

via the first VLAN, responsive to the authentication request (0053; 0067); and

forwarding the data packets received from the authorized computing device at the first

port of the packet forwarder the network via the second port of the packet

forwarder using the permanent VLAN based on the replacement IP address

assigned to the authorized computing device (0025; 0051; 0067).

Mukherjee does not explicitly disclose issuing the computing device a replacement IP address assigned to the permanent VLAN for communication with the network, responsive to receiving satisfactory authentication credentials from the computing device. Cheline, in analogous art however, disclose issuing the computing device a replacement IP address assigned to the permanent VLAN for communication with the network, responsive to receiving satisfactory authentication credentials from the computing device (0051; 0055; 0056; 0068; 0071). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Mukherjee to include issuing the computing device a replacement IP address assigned to the permanent VLAN for communication with the network, responsive to receiving satisfactory authentication credentials from the computing device. This modification would have been obvious because a person

having ordinary skill in the art would have been motivated by the desire to provide a computer implemented method for remotely configuring a Virtual Private Network (VPN) between a client-side system and a server-side system as suggested by Cheline (as suggested 0016).

Mukherjee and Cheline do not explicitly disclose blocking all data packets received at the first port of the packet forwarder from accessing the network. Kwan, in analogous art however, disclose blocking all data packets received at the first port of the packet forwarder from accessing the network (0038; 0039; 0071). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Mukherjee and Cheline to include blocking all data packets received at the first port of the packet forwarder from accessing the network. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire to provide a network device that implements a multiple key, multiple tiered system and method for controlling access to a data communications network in both a single host and multi-host environment by providing a first level of security that comprises authentication of the physical (MAC) address of a user device coupled to a port of the network device, such as a network switch, a second level of security that comprises authentication of a user of the user device if the first level of security is passed, such as authentication in accordance with the IEEE 802.1x standard, and a third level of security that comprises dynamic assignment of the port to a particular VLAN based on the identity of the user if the second level of security is passed as suggested by Kwan in (0009) .

As per claim 36:

Mukherjee disclose a computer-readable medium, wherein receiving the connection request from the unauthorized computing device requesting access to the network comprises: intercepting a request from the unauthorized computing device for a web page (figure 5: IPSG router and VISA device).

As per claim 37:

Cheline disclose a computer-readable medium, wherein: sending the unauthorized computing device the authentication request comprises directing the computing device to a network login page for authentication, the network login page accessible on the first VLAN; and wherein receiving the authentication credentials from the unauthorized computing device via the first VLAN, responsive to the authentication request comprises receiving user identification data from the unauthorized computing device based on information captured by the network login page (figure 3B: 328, 331, 332, 334).

As per claim 38:

Cheline disclose a computer-readable medium, wherein directing the unauthorized computing device to the network login page for authentication comprises: responding to the unauthorized computing device with a redirect to a Uniform Resource Locator (URL) address for the network login page (0057).

As per claim 39:

Cheline disclose a computer-readable medium, further comprising: sending the authentication credentials to a Remote Authentication Dial In User Service (RADIUS) compatible authentication server; and receiving an indication from the RADIUS compatible authentication server that the authentication credentials are authentic and that a user associated with the authentication credentials is authorized to access the network (0043; 0044).

As per claim 40:

Mukherjee disclose a system comprising:

means for receiving a connection request from an unauthorized computing device at a first port of a packet forwarder, the unauthorized computing device requesting access to a network communicably interfaced with a second port of the packet forwarder (0050; Figure 4A: 404);

means for issuing the unauthorized computing device a first Internet Protocol (IP) address assigned to a first Virtual Local Area Network (VLAN) operating within the packet forwarder and associated with the first port, wherein the first VLAN does not provide access to the network communicably interfaced with the packet forwarder via the second port, and wherein the packet forwarder blocks the data packets in the first VLAN from reaching a permanent VLAN that provides access to the network, the permanent VLAN operating within the network and associated with the second port of the packet forwarder and not the first port of the packet forwarder (Figure 2: 108; 0006; 0026; 0030; 0034);

means for sending the unauthorized computing device an authentication request through

the first port of the packet forwarder via the first VLAN based on the first IP

address, responsive to the connection request (0025; 0051; 0067);

means for issuing the authorized computing device a replacement IP address assigned to

the permanent VLAN for communication with the network and associating the

first port of the network forwarder with the permanent VLAN (0053; 0067);

means for forwarding data packets received from authorized computing device at the first

port of the packet forwarder to the network via the second port of the packet

forwarder using the permanent VLAN based on the replacement IP address

assigned to the authorized computing device (0025; 0051; 0067).

Mukherjee does not explicitly disclose means for issuing the computing device a replacement IP address assigned to the permanent VLAN for communication with the network, responsive to receiving satisfactory authentication credentials from the computing device. Cheline, in analogous art however, disclose means for issuing the computing device a replacement IP address assigned to the permanent VLAN for communication with the network, responsive to receiving satisfactory authentication credentials from the computing device (0051; 0055; 0056; 0068; 0071). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Mukherjee to include means for issuing the computing device a replacement IP address assigned to the permanent VLAN for communication with the network, responsive to receiving satisfactory authentication credentials from the computing device. This modification would have

been obvious because a person having ordinary skill in the art would have been motivated by

the desire to provide a computer implemented method for remotely configuring a Virtual

Private Network (VPN) between a client-side system and a server-side system as suggested by

Cheline (as suggested 0016).

Mukherjee and Cheline do not explicitly disclose means for blocking all data packets

received at the first port of the packet forwarder from accessing the network. Kwan, in

analogous art however, disclose means for blocking all data packets received at the first port of

the packet forwarder from accessing the network (0038; 0039; 0071). Therefore, it would have

been obvious to a person having ordinary skill in the art at the time the invention was made to

modify the method disclosed by Mukherjee and Cheline to include means for blocking all data

packets received at the first port of the packet forwarder from accessing the network. This

modification would have been obvious because a person having ordinary skill in the art would

have been motivated by the desire to provide a network device that implements a multiple key,

multiple tiered system and method for controlling access to a data communications network in

both a single host and multi-host environment by providing a first level of security that

comprises authentication of the physical (MAC) address of a user device coupled to a port of

the network device, such as a network switch, a second level of security that comprises

authentication of a user of the user device if the first level of security is passed, such as

authentication in accordance with the IEEE 802.1x standard, and a third level of security that

comprises dynamic assignment of the port to a particular VLAN based on the identity of the

user if the second level of security is passed as suggested by Kwan in (0009) .

As per claim 41:

Mukherjee disclose system, wherein receiving the connection request from the computing device requesting access to the network comprises: means for intercepting a request from the unauthorized computing device for a web page (figure 5: IPSG router and VISA device).

As per claim 42:

Cheline disclose a system, wherein: sending the unauthorized computing device the authentication request comprises means for directing the unauthorized computing device to a network login page for authentication, the network login page accessible on the first VLAN; and wherein receiving the authentication credentials from the unauthorized computing device via the first VLAN, responsive to the authentication request comprises means for receiving a user identification card from the unauthorized computing device based on information captured by the network login page (figure 3B: 328, 331, 332, 334).

As per claim 43:

Cheline disclose a system, wherein directing the unauthorized computing device to the network login page for authentication comprises: means for responding to the unauthorized computing device with a redirect to a Uniform Resource Locator (URL) address for the network login page (0057).

As per claim 44:

Cheline disclose a system, further comprising: means for sending the authentication credentials to a Remote Authentication Dial In User Service (RADIUS) compatible authentication server; and means for receiving an indication from the RADIUS compatible authentication server that the authentication credentials are authentic and that a user associated with the authentication credentials is authorized to access the network (0043; 0044).

As per claim 45:

Cheline disclose a system, wherein the authentication credentials received from the unauthorized computing device comprise user-specific credentials which are independent of hardware associated with the unauthorized computing device; and wherein authorizing the unauthorized computing device based on satisfactory authentication credentials received from the unauthorized computing device comprises authorizing a user of the unauthorized computing device based on the user-specific credentials (figure 3B: 328, 331, 332, 334; 0043; 0044).

Conclusion

6.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See the notice of reference cited in form PTO-892 for additional prior art.

7.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action.   Accordingly, **THIS ACTION IS MADE FINAL**.   See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this

final action.

Contact Information

8.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784

and fax number is (571) 273-3784. The examiner can normally be reached on 9:00am - 6:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization

where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Techane J. Gergiso/

Examiner, Art Unit 2437

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2437